Section C - Description/Specifications/Statement of Work

Statement of Work (SOW) for
Marine Gas Turbine & Propulsion Support Services

1.0 INTRODUCTION

1 0 1 The Naval Surface Warfare Center Philadelphia Division (NSWCPD) is a Department of Defense entity responsible for research and development, test and evaluation, engineering and fleet support organization for the Navy's ships, submarines, military watercraft and unmanned vehicles This requirement is for NSWCPD Code 423, which is responsible for Configuration Data Management, Engineering, Information Technology and Integrated Logistics Support Services for the Marine Gas Turbine Program, and for related HM&E Propulsion and Power Generation Machinery Systems as managed by the Propulsion Executive Steering Committee (PESC)

1 0 2 This contract is for non-personal services It does not create employment rights with the U S Government whether actual, inherent, or implied

1 0 3 Government / Contractor Relationship

(a) The services to be delivered under this Contract are non-personal services and the parties recognize and agree that no employer-employee relationship exists or will exist under the Contract/Task Order between the Government and the Contractor's personnel Therefore, it is in the best interest of the Government to provide both parties a full understanding of their respective obligations

(b) The Contractor employees shall identify themselves as Contractor personnel by introducing themselves or being introduced as Contractor personnel and displaying distinguishable badges or other visible identification for meetings with Government personnel In addition, Contractor personnel shall appropriately identify themselves as Contractor employees in telephone conversations and in formal and informal written correspondence

(c) Contractor personnel under this Contract shall not engage in any of the inherently governmental functions listed at FAR Subpart 7 5 or DFARS Subpart 207 5

(d) Employee Relationship:

1. The services to be performed under this Contract do not require the Contractor or its personnel to exercise personal judgment and discretion on behalf of the Government Rather the Contractor's personnel will act and exercise personal judgment and discretion on behalf of the Contractor
2. Rules, regulations, directives, and requirements that are issued by the U S Navy and NSWCPD under its responsibility for good order, administration, and security are applicable to all personnel who enter a Government installation or who travel on Government transportation This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract

(e) Inapplicability of Employee Benefits: This Contract/Task Order does not create an employer-employee relationship Accordingly, entitlements and benefits applicable to such relationships do not apply

(f) Notice It is the Contractor's, as well as the Government's, responsibility to monitor Contract/Task Order activities and notify the Contracting Officer if the Contractor believes that the intent of this Section has bee may be violated

1. The Contractor shall notify the Contracting Officer in writing via letter or email within three (3) calendar days from the date of any incident that the Contractor considers to constitute a violation of this Section The notice should include the date, nature, and circumstances of the conduct; the name, function, and activity of each Government employee or Contractor official or employee involved or knowledgeable about such conduct; identify any documents or substance of any oral communication involved in the conduct; and the Contractor's estimated date when, absent a response, cost, schedule or performance will be impacted
2. The Contracting Officer will, within five (5) calendar days after receipt of notice, respond to the notice in writing In responding, the Contracting Officer will either:

i. Confirm the conduct is in violation and when necessary direct the mode of further performance,
ii. Countermand any communication regarded as a violation,
iii. Deny that the conduct constitutes a violation and when necessary direct the mode of further performance, or
iv. In the event the notice is inadequate to make a decision, advise the Contractor what additional information is required, and establish the date by which it should be furnished by the Contractor

1 **BACKGROUND**

NSWCPD is responsible for providing Configuration Data Management, Engineering, Information Technology and Logistics support for Hull, Mechanical, and Electrical (HM&E) equipment on US Support includes life cycle management, program management, engineering change development, system configuration tracking, support documentation and other integrated logistics support, and Depot management Work under this solicitation is related to Marine Gas Turbine (MGT) program systems specifically, and to other systems and equipment under the purview of the Propulsion Executive Steering (PESC) in general, with the bulk of the work associated with US Navy Surface Combatant Ships Hulls also affected may include Carriers, Mine Sweeping Vessels and various Amphibious Ships and Assau (including Landing Craft (LCAC) and Ship-to-Shore Connectors (SSC)) Tasking that may be included within "HM&E machinery areas" beyond MGT Engines and Ancillary equipment include: shafting, p gears, propellers, hubs, Oil Distribution Boxes, and other prime movers associated with Ship propulsion and power generation other prime movers associated with ship propulsion and power generation Tas expected to assist NSWCPD with providing engineering and information technology services to customers beyond our traditional naval customers (i e NAVAIR, MSC, USCG, US Army, Foreign Military, e configuration and system management, maintenance, depot and logistics needs The predominant work area, however, is for U S Navy MGT related systems Support as previously noted may necessitate th variety of funding sources (RDT&E/ONR, OPN, OM&N, SCN, FMS, etc) Tasking for Risk Mitigation Framework (RFM) Support, the contractor shall produce and maintain RFM artifacts related to the au de-authorization of assigned RMF packages, applications, and systems under the cognizance of NSWCPD Cybersecurity support consists of creating and maintaining Authorization and Accreditation (A&A artifacts; creation and maintenance of the package record in the RMF system of record (currently eMASS), recommendation of security posture improvements, and Subject Matter Expertise in RMF life cyc For the purposes of this solicitation, the contractor shall be responsible primarily to provide program management, professional engineering services, and professional information technology and system pro requested to support the MGT Program and related HM&E propulsion and power generation machinery The foregoing is in support of Division 42, as directed through the Marine Gas Turbine Program Off by the PESC via Technical Instruction DIVISION 31 will provide support for integrated Logistics and Information Technology Support

2 **SCOPE OF WORK**

1 For Configuration Data Management, Engineering, Information Technology and Integrated Logistics Support Services for the Marine Gas Turbine Program, and for related HM&E Propulsion and I Machinery Systems as managed by the Propulsion Executive Steering Committee (PESC), and RMF Support system of record (currently eMass)

2.0 APPLICABLE DOCUMENTS

2 1 DoD Directive (DoDD) 8140 01, "Cyberspace Workforce Management (https://www esd whs mil/Portals/54/Documents/DD/issuances/dodd/814001p pdf)

2 2 DoD 5200 02 DoD Personnel Security Program (https://www esd whs mil/Portals/54/Documents/DD/issuances/dodi/520002p pdf)

2 3 Joint Fleet Maintenance Manual (JFMM) Volume IV Tests and Inspections (COMFLTFORCOMINST 4790 3 REV B CH-3) Section 23 (https://www navsea navy mil/Portals/103/Docume /Volume%20IV pdf)

2 4 NAVAL SHIPS' TECHNICAL MANUAL CHAPTER 234 MARINE GAS TURBINES
S9086-HC-STM-010 (https://fas org/man/dod-101/sys/ship/nstm/)

2 5 SECNAV M-5239 2 Department of the Navy Information Assurance (IA) Workforce Management Manual (https://www public navy mil/fltfor/ttgl/modules/c4i/IA%20References

/SECNAV%20M5239 2%20IAWF pdf)

2 6 DOD 4120 24-M Defense Standardization Program Policies and Procedures (https://www esd whs mil/Portals/54/Documents/DD/issuances/dodm/412024m pdf)

2 7 MIL-STD-961 Department of Defense Standard Practice Defense and Program-Unique Specifications Format and Content (https://www product-lifecycle-management com/download/MIL

The contractor shall reference and utilize the latest version available when performing tasks within this SOW

3.0. REQUIREMENTS

The contractor shall provide support to the MGT Program and the PESC through technical efforts for assigned systems including:

3 1 Provision of professional Information Technology and System Programming services in support of the MGT Information System (MGTIS)/Weblog, and associated databases for all propulsion equipment with the primary focus on 2SCOG assets including:

3 1 1 Ensuring functionality, guaranteeing database structural integrity and quality assurance, processing of all monthly updates;
3 1 2 Providing programming changes and upgrades;
3 1 3 Develop and maintain formal backup and recovery plans;
3 1 4 Develop and maintain formal testing plans;
3 1 5 Providing troubleshooting services as needed;
3 1 6 Providing Server Support in maintaining the NSWCPD servers in the NMCI or NGEN or other hosting environment including SPAWAR and DISA, and troubleshooting data transmittal probl servers
3 1 7 Provide cybersecurity support including:

a) Maintain the Authority to Operate (ATO) through the Authorization and Accreditation (A&A) process and associated documentation required to meeting A&A requirements Risk Mitigation Fran
b) Maintaining a high speed internet connection to the servers;
c) Perform regular administrative functions;
d) Perform monthly data backups;
e) Restoration of servers after any hardware or software problem;
f) Adding any software patches needed to maintain server operations and flow of data;
g) Maintain other database connections as required including CDMD-OA; and
h) The contractor must further provide web access to the database for direct, NSWCPD specified edit/update capabilities for NSWCPD specified activities

NOTE: Contractor personnel accessing information systems shall meet applicable training and certification requirements set forth in DoD 8570 01M, DOD5200 2-R, and SECNAV M-523 responsible to ensure that personnel possess and maintain the proper and current Information Assurance (IA) certifications in accordance with DoD 8570 01M and the Computing Environment/Ope certifications in accordance with SECNAV M-5239 2 See Section 8 of this SOW for the Cybersecurity Workforce / Information Assurance Workforce Contractor Training Requirements Matrix

3 1 8 Providing DBA support in maintaining the integrity of all databases and the functionality of the MGTIS/Weblog, and any needed interface functionality and reporting mechanisms specified
3 1 9 Maintain data models and Functional Design Documentation (FDD)
3 1 10 Maintain and revise, as required MGTIS training and Help System
3 1 11 Perform data audits utilizing SQL queries, as required to identify user generated data errors, duplicate information, and increase data quality and data accuracy

NOTE: At the completion of the period of performance work, the contractor shall deliver any and all MGTIS/Weblog programming, code, applets, scripts, queries, data files, hardware, FDI software/hardware contract, or licensing documentation in accordance with CDRL A005

3 2 Development, administration, and maintenance of database systems to support program management needs Related to this, the contractor must:

3 2 1 Provide data updates as needed to the US Navy Integrated Propulsion and Auxiliary Power Generation Portal (NIPPGP) Website, as authorized by the PESC and user community where appli

a) Develop and maintain data models and Functional Design Documentation (FDD)
b) Develop and maintain formal backup and recovery plans
c) Ensuring functionality, guaranteeing database structural integrity and quality assurance, processing of all monthly updates;
d) Providing DBA support in maintaining the integrity of all databases and the functionality of the Propulsion Portal, and any needed interface functionality and reporting mechanisms specified
e) Providing troubleshooting services as needed;
f) Perform review of system generated 3M files and submit reviewed files to Type Commander (TYCOM) as required
g) Maintain other database connections as required including CDMD-OA
h) Maintain the Authority To Operate (ATO) through the Assessment and Authorization (A&A) process and associated documentation required to meeting A&A requirements;

NOTE: At the completion of the period of performance work, the contractor shall deliver any and all MGTIS/Weblog programming, code, applets, scripts, queries, data files, hardware, FDD, and s contract, or licensing documentation in accordance with CDRL A005

3 3 The contractor shall produce and maintain Risk Mitigation Framework (RMF) artifacts related to the authorization or de-authorization of assigned RMF packages, applications, and systems und NSWCPD Cybersecurity support consists of creating and maintaining A&A packages and artifacts; creation and maintenance of the package record in the RMF system of record (currently eMASS security posture improvements, and Subject Matter Expertise in RMF life cycle management The contractor shall coordinate with system representatives via all avenues necessary to facilitate and a to support this action The intended result is obtaining or maintaining Authorization to Operate (ATO) or De-Authorization to Operate (DATO) through validated test results, security controls asses authorization official endorsement

All RMF activities shall follow the most current applicable documents including: DON RMF Process Guide (RPG), DoD Instruction 8510 01, and the business rules of cognizant review of Tasks include:

1. Proper documentation of residual risks in a plan of actions and milestones formatted in compliance with the current package system, currently eMASS
2. Tracking of deliverables and action items in accordance with A&A guidance
3. Ensure package compliance with stated of existing DON and DoD policies
4. Manage, attend, and support configuration control board practices
5. Maintain current vulnerability scan data and residual risk plan of actions and milestones in Vulnerability Remediation Asset Manager (VRAM)
6. Perform risk management and security engineering for Zone D boundaries to include IAVM support, remediation, patching, scanning and associated boundary maintenance
7. Develop all required eMASS documents, to include Plan of Actions and Milestones (POA&Ms)/ Risk Assessment Reports (RARs) and DISA Security Technical Implementation Guides (STIGs); products shall be created in the appropriate software (i e Microsoft Visio, scanning software, eMASS DISA STIG Viewer, etc)
8. Determine a system's compliance with all applicable Controls and Assessment Procedures (APs) for an assigned DoN system, including developing the appropriate test procedures, if necessary; executing the test procedures; and accurately documenting the results of security testing The A&A Analysts shall update the eMASS record for the assigned system(s);
9. Ensure RMF artifacts are in compliance with published Navy, NAVSEA Business Rules (OPNAV N2N6 and/or NAVSEA), NIST SP-800-37 and SP-800-53 Rev 4 In addition, local NSWCPD policies and procedures may apply Command Information System Security Manager (ISSM) will resolve any conflicting interpretations;
10. Collect and collate system or site information and use it to evaluate and document in eMASS the security posture of the IT system or site being Assessed, Authorized, and maintained;
11. Review security assessment plans, test plans, and procedures to ensure they addresses the correct level of effort and are sufficiently comprehensive to assess all IA requirements applicable to the IT system or site, for assessment, authorization, and maintenance have been met;
12. Optimize A&A testing procedures to ensure the most accurate reporting in the appropriate format and that all IA requirements have been addressed Evaluate all discrepancies and recommend potential mitigation measures for reducing or eliminating specific risks;
13. Work with the Information System Owner/ISSO/System Administrators equivalent to NSWCPD's Information System Security Officer (ISSO) to determine applicable fixes and/or mitigation for weaknesses and to determine

the adequate level of residual risk;

14. Create and verify the accuracy of POA&Ms/RARs as identified by vulnerability actual test results;
15. Ensure information systems are operated, used, maintained, and disposed of in accordance with security policies and practices as required by the authorization package and NSWCPD

NOTE: At the completion of the period of performance work, the contractor shall deliver any and all MGTIS/Weblog programming, code, applets, scripts, queries, data files, hardware, FDD, and software/hardware contract, or licensing documentation in accordance with CDRL A007

3 4 Engineering services include research and recommendations for correcting CS non-compliance findings Tasking includes reviewing and analyzing network security requirements, information system design, and softwar and hardware, as well as analysis to ensure security controls are implemented in compliance with CS policies and standards (i e DOD, DON, NAVSEA, and Command-level cybersecurity policies, instructions, NIST SP-800-37 Risk Management Framework lifecycle and NIST SP-800-53 R4 Information System Security Controls, OPNAV N2N6) Contractor shall support each of the following areas by:

1. Supporting the A&A Program for Assigned Systems:

   Ensuring accreditation and authorization packages for systems within the assigned technical department are developed, maintained, and updated prior to the operation date (minimum 5 working days) and/or expiratic (minimum 5 working days)
2. Supporting the Command Information System Security Manager (ISSM):

   Working with ISSM to tailor the delivery of Cybersecurity Program elements, such as accreditation requirements and strategies, to ensure effective dissemination and implementation within the assigned technical department, at least weekly Ensures information systems are operated, used, maintained, and disposed of in accordance with security policies and practices as required by the authorization package and NSWCPD Manages and implements the cybersecurity process, and oversees weekly documentation in accordance with the Risk Management Framework (RMF) to obtain assigned system's, enclaves, and boundaries Authority Operate (ATO) Tracks and reports on production of system cybersecurity artifacts and status of cybersecurity Assessment & Authorization (A&A) efforts (per week) Review, evaluate, and audit user access request behalf of the ISSM
3. Perform and Document Risk Assessments and Vulnerability State:

   On a quarterly basis, examine system services and provide guidance to users in assigned department on disabling services, reviews vulnerability findings with SMEs to determine potential impact of remediation effo devises system remediation and associated test procedures based on vulnerability scan results, STIG findings, and review of system services
4. Prepare and present accurate briefing materials to customers, government, and contractor personnel as directed to provide status, respond to inquiries, and disseminate technical information Correspondence and briefing materials are logically structured and contain sufficient background to clearly convey their intended message Drafts are provided for supervisory review on or before 3 working days prior to deadline
5. Coordinate/conduct cybersecurity vulnerability analysis and threat assessments (at least monthly) that are accurate in regards to the architecture of RDT&E IT assets/systems (per ATO) and ship platforms/systems (per ATO) Works weekly with individual system Subject Matter Experts (SME) to determine cybersecurity requirements, designs, and migration paths for assigned programs
6. Policies, procedures and decision-making processes center on requirements, program risk, and customer satisfaction Contractor shall promote two-way communication weekly with customers and uses multiple forums to communicate services provided, assessed risk, and gather feedback

NOTE: At the completion of the period of performance work, the contractor shall deliver any and all MGTIS/Weblog programming, code, applets, scripts, queries, data files, hardware, FDD, and software/hardware contract, or licensing documentation in accordance with CDRL A007

3 5 Contractor shall assist in the preparation of systems for the accreditation process by making systems compliant; to include implementation of DISA's Security Technical Implementation Guide (STIG) and patchin system assets to current acceptable levels, researching and providing recommendations for correcting CS non-compliance findings Tasking includes reviewing and analyzing network security requirements, network and software and hardware Other tasking includes analysis to ensure security controls are implemented in compliance with CS policies and standards The contractor shall ensure that the requirements are effectively integrated into information technology component products and information systems through purposeful security architecting, design, development, and configuration Information system security engineers are an in part of the development team (e g , integrated project team) designing and developing organizational information systems or upgrading legacy systems Information system security engineers employ best practices w implementing security controls within an information system including system/security engineering principles System security engineers coordinate their security-related activities with information system owners, a information system security officers Contractor shall support in each of the following areas by:

3 5 1 Ensuring accreditation and authorization packages for systems within the assigned technical department are developed, maintained, and updated prior to the operation date (minimum 5 working days) and/or expiration date (minimum 5 working days), and on a continual basis as required by the DON RMF Process Guide Ensures hardware and software inventories are accurate and up to date in the inventory systems and system of record, eMASS Identifies the security control baseline set, and any necessary tailoring Assists with the development, maintenance, and tracking of the system security plan and the corresponding risk assessment report (RAR) Assists with any required security testing required as part of the A&A Program or continual monitoring program including vulnerability scans utilizing ACAS, antivirus scans, and configur compliance maintenance (e g STIGs) Maintains all required eMASS documents, to include (but not limited to) Plan of Actions and Milestones (POA&Ms)/ Risk Assessment Reports (RARs) and DISA Security Tec Implementation Guides (STIGs)

3 5 2 As required by RMF documentation and continuous monitoring requirements, examining system services and provide guidance to users in assigned department on disabling services, reviews vulnerability find with SMEs to determine potential impact of remediation efforts, and implements system remediation and associated test procedures based on vulnerability scan results, STIG findings, and review of system services on remediation plans, applies appropriate patches to maintain ATO on a quarterly basis Analyze and ensure ACAS vulnerability scans are accurate, credentialed, and is uploaded to the system of record currently the Vulnerability Remediation Asset Manager (VRAM)

3 5 3 Prepares and presents accurate briefing materials to customers, government, and contractor personnel as directed to provide status, respond to inquiries, and disseminate technical information Correspondence and brie materials are logically structured and contain sufficient background to clearly convey their intended message Drafts are provided for supervisory review on or before 3 working days prior to deadline

3 5 4 Coordinates/conducts cybersecurity vulnerability analysis and threat assessments (at least monthly) that are accurate in regards to the architecture of RDT&E IT assets/systems (per ATO) and ship platforms/systems (p ATO) Works weekly with individual system Subject Matter Experts (SME) to determine cybersecurity requirements, designs, and migration paths for assigned programs

NOTE: At the completion of the period of performance work, the contractor shall deliver any and all MGTIS/Weblog programming, code, applets, scripts, queries, data files, hardware, FDD, and software/hardware contract, or licensing documentation in accordance with CDRL A007

3 6 Upon the issuance of Technical Instructions (T I 's), to be issued by the Contracting Officer identified under this Seaport Order, the contractor shall support technical and systems analysis tasks as specified below Performance of the requirements will be at NSWCPD, and at the contractor's facilities Some of the work requires temporary travel to worldwide locations as specified under Paragraph 3, contained herein Actual tas will be defined under applicable T I 's

3 6 1 The contractor shall provide technical services such as engineering technician support functions for NSWCPD Code 423 to accomplish various propulsion and auxiliary gas turbine program projects

3 6 2 The contractor shall provide technical support for the LM2500 and 501K-17/34 and other MGT engine borescope programs such as providing technician services using borescope equipment to assist in the eval and diagnosis of internal engine conditions, and to prepare technical reports to document findings of such inspections on USN Surface Ships, US Coast Guard Ships, Military Sealift Command Vessels and Foreign M Ships

3 6 3 The contractor shall provide technical support for the LM2500 Digital Fuel Control program and other MGT engine line programs such as providing technical assistance with back fitting approved engine configuration changes, pre-assembly of kits and other mechanical and/or electrical installation support as requested on US Navy Surface Ships, US Coast Guard Ships, as well as Foreign Military Vessels Support wi include authorization/certification of a journeyman engineer technician to be fork truck operator certified to provide assistance on an as required basis for kitting and material transfer needs

3 6 4 The contractor shall provide in-service engineering support for the LM2500 and 501K-17/34 gas turbine engines and other Marine Gas Turbine Engines supporting the Navy Marine Gas Turbine Program; supp includes Special Support Equipment (SSE) used by the fleet to maintain and service gas turbine engines

3 6 5 The contractor shall Schedule and coordinate annual LM2500 Coast Guard shipboard organizational level maintenance and training for the Maritime Security Cutter – Large (WMSL) Class Cutter

3 6 6 The contractor shall Interface with Surface Warfare Officer Schools (SWOS) headquarters and subordinate commands to participate and provide feedback for Technical Training Audits for all USN gas turbine training

3 6 7 The contractor shall Coordinate and conduct onsite Organizational (“O”) and Intermediate (“I”) level gas turbine training for Foreign Military Sales (FMS) program and USN military students

3 6 8 The contractor shall manage NSWCPD onsite material inventory to include Digital Fuel Control (DFC), Decom, and MGT Kits

3 6 9 The contractor shall participate in annual training and SSE audit of “I” level activities such as Norfolk Ship Support Activity (NSSA), Southeast Regional Maintenance Center (SERMC), and Southwest Region Maintenance Center (SWRMC)

3 6 10 The contractor shall maintain and update LM2500 and other MGT configuration and technical directive installation plans as directed

3 6 11 The contractor shall manage the Building 1000 physical inventory

3 6 12 The contractor shall coordinate and provide detailed estimates for FMS requests submitted to NSWCPD Code 4230

4.0 DATA REQUIREMENTS

4.1 Contract Status Report (CDRL A001)

4 1 1 This report shall reflect both prime and Subcontractor data if applicable at the same level of detail
4 1 2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable the Government's approval must be received in writing from the COR within 5 business days before submission

4.2 Travel Report (CDRL A002)

4 2 1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail
4 2 2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor’s format is acceptable, Government’s approval is required from the COR

4.3 Contractor’s Personnel Roster (CDRL A003)

4 3 1 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor’s format is acceptable, Government’s approval is required from the COR This report shall reflect both prime and subcontra data if applicable at the same level of detail

4.4 Other Direct Costs Report (CDRL A004)

4 4 1 The CDRL shall be delivered electronically, unless otherwise stated or data is being submitted in eCRAFT, and while Contractor’s format is acceptable, Government’s approval is required from the COR This report reflect both prime and subcontractor data if applicable at the same level of detail

4.5 Software Components (CDRL A005)

4 5 1 Original source code (un-compiled) for information technology efforts for all work associated with SOW Section 3 1 & 3 2, monthly
4 5 2 Programming, code, applets, scripts, queries, data files, hardware, FDD, and software/hardware contract, or licensing documentation for all work associated with but not limited to section 3 1 & 3 2, quarterly

4.6 Contractor Financial Analysis Reports (CDRL A006)

4 6 1 The Burn Rate Analysis Report is a summary report that captures the rate at which the money is expended This report shall be attached in Wide Area Workflow Receipts and Acceptance (WAWF-RA), beginning th (30) days after award and every thirty (30) days thereafter
4 6 2 The Incurred Costs Report is a report that captures a summary of all costs incurred to date This report shall be attached in Wide Area Workflow Receipts and Acceptance (WAWF-RA), beginning thirty (30) days af award and every thirty (30) days thereafter

4.7 DOD Risk Management Framework (RFM) Package Deliverables (CDRL A007)

4 7 1 For information technology efforts for all work associated SOW Section 3 3, 3 4, & 3 5 monthly
4 7 2 An RMF package artifacts shall contain the necessary artifacts required by the DAA, NAO, AO, or ISSM to successfully achieve Platform IT (PIT) Designation, Platform IT Risk Approval (PRA), Interim Authorit (IATT), or Authority to Operate (ATO)

4.8 Quality Management System (QMS) (CDRL A008)

4 8 1 Contractor shall deliver a QMS in accordance with SOW Section 10 0 within twenty- one (21) days of date of Task Order award

5.0 SECURITY REQUIREMENTS

5 1 Contractor is responsible for completing all required Government mandated training to maintain security and network access to government sites and IT systems to include but not limited to: Antiterrorism Level 1 Awareness; DoD Cyber Awareness Challenge; Combatting Human Trafficking; Records Management in the DON: Everyone's Responsibility; Training and Readiness: The Active Shooter; Constitution Day; NAVSEA Introduction to Controlled Unclassified Information; Operations Security (OPSEC); NAVSEA Counterintelligence Training; Privacy and Personally Identifiable Information (PII) Awareness Training; and NAVSEA Physical Security training Certificates of successful completion shall be sent to the COR and as otherwise specified in the contract

5.1.1 In accordance with the NISPOM DoD 5220 22M, Contractor personnel that require access to Department of Navy (DON) information systems and/or work on-site require an open investigation or favorable adjudicated Tier 3 by the Vetting Risk Operations Center (VROC) An interim clearance is granted by VROC and recorded in the Joint Personnel Adjudication System (JPAS) An open or closed investigation with a favorable adjudication is required prior to issuance of a badge providing access to NSWCPD buildings Furthermore, if the Navy Central Adjudication Facility, have made an unfavorable determination access will be denied For Common Access Card (CAC) you must have an open investigation and or favorable adjusted investigation Interim security clearance are acceptable for a CAC Access will be denied for anyone that has eligibility pending in JPAS Vetting through the National Crime Information Center, Sex Offender Registry, and the Terrorist screening database shall be process for a contractor that does not have a favorable adjudicated investigation

5.1.2 Contractor personnel that require a badge to work on-site at NSWCPD must provide an I-9 form to verify proof of citizenship The I-9 form should be signed by the company Facility Security Officer or the company Human Resource Department In addition to the I-9 form, Contractors shall also bring their birth certificate, current United States Passport or naturalization certificate and state issued ID to the NSWCPD Security Officer at the time of badge request to verify citizenship Any contractor that has unfavorable information that has not been favorably adjudicated, by Department of Defense Central Adjudication Facility (DOD CAF) will not be issued a badge

5.1.3 Within 30 days after contract award, the contractor shall submit a list of all contractor personnel, including subcontractor employees, who will have access to DON information systems and/or work on-site at one of the NSWCPD sites to the appointed Contracting Officer Representative (COR) via email The contractor shall provide each employee's first name, last name, contract number, the NSWCPD technical code, work location, whether or not the employee has a CAC and or Standard Access Control Badge (SACB), the systems the employee can access (i e , NMCI, RDT&E), and the name of the Contractor's local point of contact, phone number and email address Throughout the period of performance of the contract, the Contractor shall immediately provide any updated information to the COR when any Contractor personnel changes occur including substitutions or departures

This effort may require access to classified information up to the Secret level No classified data will be generated or stored by the Contractor As per the direction/discretion of the COR, certain contract personnel will be required to have and maintain a SECRET clearance while some may only need CONFIDENTIAL The requirements of the attached DD Form 254 apply

The Contractor shall appoint a Facility Security Officer (FSO), who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industrial Security Program Operating Manual (NISPOM) (DOD 5220 22-M), and (3) assure compliance with any written instructions from the NSWCPD, Security Office

The Prime Contractor shall:

1. Forward signed copies of DD254s provided to subcontractors to the Naval Surface Warfare Center Philadelphia Division (NSWCPD), ATTN: Security
2. Direct the subcontractor to obtain approval, through the prime Contractor, for the public release of information received or generated by the sub through the prime Contractor
3. Submit the subcontractor request for public release through the technical point of contact identified on the DD 254

Additional information related to the facility clearance process can be obtained by visiting www.dss.mil or http://www.dss.mil/isec/pcl_index.htm.

The planned utilization of non-U S Citizens in the performance of this contract effort must be identified by name and country of citizenship in the proposal Foreign Nationals shall not be allowed access to classifiec critical program information unless approved on a case by case basis by DSS

5.4 OPERATIONS SECURITY (OPSEC)

5.4.1 The Contractor shall protect critical information associated with this contract to prevent unauthorized disclosure The NSWC Philadelphia Division's (NSWCPD) Critical Information List (CIL)/ CIIL (Critical Indicators and information list) will be provided on site, if warranted Performance under this contract requires the contractor to adhere to OPSEC requirements The Contractor may not impose OPSEC requirements on its subcontractors unless NSWCPD approves the OPSEC requirements During the period of this contract, the Contractor may be exposed to, use, or produce, NSWCPD Critical Information (CI) and/or observables and indicators which may lead to discovery of CI NSWCPD's CI will not be distributed to unauthorized third parties, including foreign governments, or companies under Foreign Ownership, Control, or Influence (FOCI)

5.4.2 CUI correspondence transmitted internally on the contractor's unclassified networks or information systems, and externally, shall be protected per NIST SP-800-171, Protecting Controlled Unclassified Information (CUI) in Non-federal Systems and Organizations

Assembled large components/systems being transported to and from testing areas, other production or government facilities (whether or not on public roadways) shall be in an enclosed van trailer or covered flatbed trailer Component/System outside storage, staging, and test areas shall be shielded/obscured from public view wherever physically possible

5.4.3 NSWCPD's CI shall not be publicized in corporate wide newsletters, trade magazines, displays, intranet pages or public facing websites Media requests related to this project shall be directed to the PCO, and the COR who will forward the required to the NSWCPD Public Release Authority for review

5.4.4 Any attempt by unauthorized third parties to solicit, obtain, photograph, or record, or; incidents of loss/compromise of government Classified or CI, Business Sensitive, Company Proprietary information related to this or other program must be immediately reported to the contractor's Facility Security Officer and Cognizant Security Office and/or the Naval Criminal Investigative Service, and the NSWC PD Security Division (Code 105 1) Questions concerning these requirements shall be directed to the PCO, and the COR who will forward the request to the NSWC PD Security Division (Code 105 1)

5.5 RECEIPT, STORAGE, AND GENERATION OF CONTROLLED UNCLASSIFIED INFORMATION (CUI)

All Controlled Unclassified Information (CUI) associated with this contract must follow the minimum marking requirements of DoDI 5200 48, Section 3, paragraph 3 4 a, and include the acronym "CUI" in the banner and footer of the document In accordance with DoDI 5200 48, CUI must be safeguarded to prevent Unauthorized Disclosure (UD) CUI export controlled technical information or other scientific, technical, and engineering information must be marked with an export control warning as directed in DoDI 5230 24, DoDD 5230 25, and Part 250 of Title 32, CFR Nonfederal information systems storing and processing CUI shall be protected per NIST SP-800-171, or subsequent revisions All transmissions to personal email accounts (AOL, Yahoo, Hotmail, Comcast, etc) and posting on social media websites (Facebook, Instagram, Twitter, LinkedIn, etc) are prohibited Destroy CUI associated with this contract by any of the following approved methods: A cross-cut shredder; a certified commercial destruction vendor; a central destruction facility; incineration; chemical decomposition; pulverizing, disintegration; or methods approved for classified destruction

6.0 PLACE OF PERFORMANCE

To ensure support is available as required the contractor must be in the Region/Zone of the Philadelphia Naval Business Center and not require more than local travel orders for the Program representatives to visit th contractor's facility The contractor's facility must have adequate capabilities (floor space, high speed data connectivity, computers, telephones, conference room(s) and printers) to fully support the SOW At least 50% the work under this task is to be performed at the contractor's local regional office location Contractor must be able to be physically present at server location/government owned facilities/PNBC within one (1) hour request for assistance:

6 1 Performance that occurs at the government site will be subject to the following guidelines:

6 1 1 The Government will provide cubicles (i e , Office, etc) and necessary phone/computer equipment for up to (8) contractor personnel, as specified in Section 8 0 of this document, as needed/requested to comple specific task order items

6 1 2 The specific location(s) will be provided at time of award of the Task Order The Contractor shall provide a list of employees who require access to these areas, including standard security clearance information each person, to the Contracting Officer Representative (COR) no later than three business days after the date of award The work space provided to the Contractor personnel shall be identified by the Awardee, with appropriate signage listing the company name and individual Contractor employee name

6 1 3 Access to Government buildings at Naval Surface Warfare Center Philadelphia Division is from 0600 to 1800 Monday through Friday, except Federal holidays Normal work hours are from 0600 to 1800, Mon through Friday Contractor employees shall be under Government oversight at all times Government oversight requires that a Government employee be present in the same building/facility whenever Contractor employee(s) are performing work under this Contract/Task Order Contractor personnel are not allowed to access any Government buildings at NSWCPD outside the hours of 0600 to 1800 without the express appro the Procuring Contracting Officer (PCO)

6 1 4 Early Dismissal and Closure of Government Facilities

When a Government facility is closed and/or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contract personnel regularly assigned to work at that facility should follow the same reporting and/or departure directions given to Government personnel The Contractor shall not direct charge to the contract for time off, bu follow its own company policies regarding leave Non-essential Contractor personnel, who are not required to remain at or report to the facility, shall follow their parent company policy regarding whether they shoul go/stay home or report to another company facility Subsequent to an early dismissal and during periods of inclement weather, onsite Contractors should monitor radio and television announcements before departing work to determine if the facility is closed or operating on a delayed arrival basis

When Federal employees are excused from work due to a holiday or a special event (that is unrelated to severe weather, a security threat, or a facility related problem), on site Contractors will continue working estab work hours or take leave in accordance with parent company policy Those Contractors who take leave shall not direct charge the non-working hours to the Contract/Task Order Contractors are responsible for predetermining and disclosing their charging practices for early dismissal, delayed openings, and closings in accordance with the FAR, applicable cost accounting standards, and company policy Contractors shall fo their disclosed charging practices during the Contract/Task Order period of performance, and shall not follow any verbal directions to the contrary The PCO will make the determination of cost allowability for time due to facility closure in accordance with FAR, applicable Cost Accounting Standards, and the Contractor's established accounting policy

6 1 5 The contractor shall ensure that each contractor employee who will be resident at NSWCPD completes the Environmental Management System (EMS) Awareness training within 30 days of commencing perfo at NSWCPD This document is available at: https://navsea navy deps mil/wc/pnbc-code10/Safety/default aspx

In accordance with C-223-W002, ON-SITE SAFETY REQUIREMENTS (NAVSEA), the contractor shall certify by e-mail to (b)(6) that on-site employees have read the "Philadelp Division Environmental Policy and Commitment" and taken the EMS Awareness training within 30 days of commencing performance at NSWCPD The e-mail shall include the employee name, work site, and contr number

7.0 TRAVEL

The Contractor may be required to travel from the primary performance location when supporting this requirement It is anticipated that 50% of this effort will be conducted at the NSWCPD facility in Philadelphia, and the remaining 50% of the effort conducted at Contractor Facilities or while on temporary travel Travel will be required to support: kit distribution; Ship and TYCOM waterfront interface requirements (on occas and only as requested); for various inspections and installation support work for the MGT Program; for MGT Inspector refresher training sessions; and software development conferences Trips will be determined as situations arise The need for Local travel is not anticipated Travel requirements may result in travel of up to 69 days for approximately 10 trips

3 Trips of 5 day length to Norfolk, VA

3 Trips of 12 day length to San Diego, CA
2 Trips of 5 day length to Pascagoula, MS

The number of times the Contractor may be required to travel to each location cited above may vary as program requirements dictate, provided that the total estimated travel cost is not exceeded The numbers of trip types of personnel traveling shall be limited to the minimum required to accomplish work requirements All travel shall be approved by the COR and Contracting Officer before travel occurs Approval may be via th Technical Instruction (TI) In accordance with the TI instructions, before initiating any travel the Contractor(s) shall submit a detailed and fully-burdened estimate that includes the number of employees traveling, the expected travel costs for airfare, lodging, per diem, rental car, taxi/mileage and any other costs or actions requiring approval The travel estimate shall be submitted to the Contracting Officer's Representative (COR) Contract Specialist Actuals cost, resulting from the performance of travel requirements, shall be reported as part of the Contractor's monthly status report The reportable cost shall also be traceable to the Contractor invoice

All travel shall be conducted in accordance with FAR 31 205-46, Travel Costs, and B-231-H001 Travel Cost (NAVSEA) and shall be pre-approved by the COR The Contractor shall submit travel reports in accordan with DI-MGMT-81943 (CDRL A002)

Travel Costs

The current “maximum per diem” rates are set forth in the (i) Federal Travel Regulations for travel in the Continental United States; (ii) Joint Travel Regulations for Overseas Non-Foreign areas (e g , Alaska, Hawaii Guam, Puerto Rico, etc); and (ii) Department of State (DOS) prescribed rates for foreign overseas locations

8.0 PERSONNEL

8 1 Personnel Requirements All persons proposed in key and non-key labor categories shall be U S citizens holding, or having ability to obtain within 6-months of hire, a security clearance at or above the level dictat the Personnel Security Requirements in this Section

Clause 52 222-2 "Payment for Overtime Premiums" will provide for the total approved dollar amount of overtime premium or will state “zero” if not approved If overtime premium has not been approved under this contract in accordance with Clause 52 222-2, overtime effort to be performed shall be requested from the Contracting Officer prior to performance of premium overtime For overtime premium costs to be allowable the Contracting Officer is required to approve the performance of overtime prior to the actual performance of overtime The dollar amount in FAR 52 222-2 shall equal overtime premium negotiated between the Government and the prime contractor This overtime premium amount shall equal the prime contractor's unburdened premium OT labor costs plus the subcontractors' fully-burdened premium OT labor costs

The contractor workforce remains governed by DoDM 8570 01

The Level of Effort (LOE) for the performance of the resultant Task Order is based on the following labor categories and hours per year:

Title	eCRAFT Code	GOVT/KR-Site	Hrs.
Program/Project Manager II*	MANP2	KR	1500
Computer Systems Analyst III*	14103	KR	1920
Computer Programmer II*	14072	KR	3840
Specialist, Information Assurance Compliance I*	SIAC1	KR	1920
Systems Administrator II*	SA2	GOVT	1920
Computer Programmer I*	14071	KR	1920
Computer Programmer III	14073	KR	1920
Computer Programmer I	14071	KR	1920
Computer Systems Analyst II	14102	KR	1920
Specialist, Information Assurance Compliance II	SIAC2	GOVT	1920
Specialist, Information System Security III	SISS3	GOVT	1920
Specialist, Information System Security II	SISS2	GOVT	1920
Systems Administrator II	SA2	GOVT	1920
Machinery Maintenance Mechanic I	23530	GOVT	1920
Machinery Maintenance Mechanic II	23530	GOVT	1920
Supply Technician	01410	GOVT	1920
		TOTAL PER YEAR	**32220**

(*) Denotes Key Personnel

Cybersecurity Workforce / Information Assurance Workforce Contractor Training Requirements Matrix

Labor Category	Task Area	IA Duties	IAT or IAM	Level (I,II,III)	IAWF Baseline Certification (one of the listed is required)	Computing Environment Certification (for IATs only	Continuing Education Requirements
Systems Administrator II	3 1 5, 3 1 6, 3 1 7, 3 5	Information System Security Engineer (ISSE)	IAT	II	CCNA Security, CySA+ **, GIC SP, G SEC, Security + CE, SSCP Security + CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Specialist, Information Assuranc Compliance I	3 3	RMF Specialist	IAM	I	CAP, GSLC, Security+ CE	Directed by the Privileged Access Agreement	40 CPEs annually
Specialist, Information Assuranc Compliance II	3 3	RMF Specialist	IAM	I	CAP, GSLC, Security+ CE	Directed by the Privileged Access Agreement	40 CPEs annually
Specialist, Information System Security III	3 4	Information System Security Officer III	IAM	II	CAP, CASP+ CE, CISM, CISSP (or Associate), GSLC, CCISO	Directed by the Privileged Access Agreement	40 CPEs annually
Specialist, Information System Security II	3 4	Information System Security Officer II	IAM	I	CAP GSLC Security+ CE	Directed by the Privileged Access Agreement	40 CPEs annually

Computer Programmer I	3 1 1-3 1 6 & 3 1 8 – 3 1 11 & 3 2 1a – 3 2 1g	Software and DB updates	IAT	I	Security+ CE, A+ CE, CCNA-Security, Network+ CE, SSCP	None- No Privileged Access	As required to maintain certification
Computer Programmer II	3 1 1-3 1 6 & 3 1 8 – 3 1 11 & 3 2 1a – 3 2 1g	Software and DB updates	IAT	I	Security+ CE, A+ CE, CCNA-Security, Network+ CE, SSCP	None- No Privileged Access	As required to maintain certification
Computer Programmer III	3 1 1-3 1 6 & 3 1 8 – 3 1 11 & 3 2 1a – 3 2 1g	Software and DB updates	IAT	II	Security+ CE, CCNA Security, GICSP, GSEC, SSCP	None- No Privileged Access	As required to maintain certification
Computer Systems Analysts II	3 1 1-3 1 6 & 3 1 8 – 3 1 11 & 3 2 1a – 3 2 1g	Software and DB updates	IAM	I	Security+ CE, CAP, GSLC	None- No Privileged Access	As required to maintain certification
Computer Systems Analysts III	3 1 1-3 1 6 & 3 1 8 – 3 1 11 & 3 2 1a – 3 2 1g	Software and DB updates	IAM	II	CAP, CASP+ CE, CISM, CISSP (or Associate), GSLC, CCISO	None- No Privileged Access	As required to maintain certification

DFARS 252 239-7001 is applicable for this requirement

DFARS 252 239-7001 INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION (JAN 2008)

(a) The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570 01 Information Assurance Workforce Improvement Program The Contractor shall meet the applicable information assurance certification requirements, including—

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570 01-M; and

(2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570 01-M

(b) Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions

(c) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions

NOTE - CONTRACTORS *MUST* PROVIDE PROOF OF EMPLOYEE CERTIFICATION REQUIREMENTS AS DEFINED IN THE CYBERSECURITY WORKFORCE MATRIX AT THE TIME C PROPOSAL SUBMISSION. ADDITONALLY, APPENDIX A HAS BEEN UPDATED. SEE BELOW.

8.1.1 Key Personnel

The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this Task Order in accordance with Clause 52 237-3 Continuity of Services (Jan 1991) in the basic SeaPort contract The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor

In accordance with C-237-H002 Substitution of Key Personnel, the following labor categories are designated as the target Key Personnel for this contract Resumes will be submitted for each category in the quantities indicated by the key category description Target qualifications are listed below for each education and work experience qualifications for each key personnel labor category The proposed combined expertise of all proposed key personnel shall cover at a minimum all requirements for task areas 3 1, 3 2, 3 3, and 3 5 in the performance work statement

In the performance of this effort, the Contractor shall fully staff the key positions listed below with qualified individuals The Contractor shall provide individuals to fill the non-key positions as needed:

Program/Project Manager (MANP2)(one resume required):

Target Education: Bachelor's Degree in any technical or managerial discipline

Target Experience: Ten (10) years of experience in Program Management

Security Requirement: SECRET Clearance

Computer Systems Analyst III (14103)(one resume required):

Target Education: Bachelor's Degree in Computer Science, Information Technology, or an equivalent technical field

Target Experience: Seven (7) years of experience with developing web applications, technical software documentation, database administration, and programming is necessary Resume should clearly demonstrate experience with Microsoft ASP NET technologies in addition to experience with C# programming language, MSSQL, Java Script, and HTML 5 Additionally, experience as a team's senior technical resource throughou software development life cycle

MINIMUM IA Workforce Baseline: (1) of the following certifications: CAP, CASP+ CE, CISM, CISSP (or Associate), GSLC, CCISO

Security Requirement: SECRET Clearance

Computer Programmer II (14072)(two resumes required):

Target Education: Bachelor's Degree in Computer Science, Information Technology, or an equivalent technical field

Target Experience: Three (3) years of experience with programming applications and database back ends Debugging and correcting software errors in existing systems Familiarity with web-based application design an development

MINIMUM IA Workforce Baseline: (1) of the following certifications: Security+ CE, A+ CE, CCNA-Security, Network+ CE, SSCP

Security Requirement: SECRET Clearance

Specialist, Information Assurance Compliance I (SIAC1) (one resume required):

Target Education: Bachelor's Degree in Computer Science, Information Technology, or an equivalent technical field or CNSSI 4011 Certificate or successful completion of military training course: NEC 2791 (A-150-19

or K-150-2115) or IP BASIC (CIN: J-3B-0440) (or DOD Service equivalent)

Target Experience: One (1) to three (3) years of experience with tasks in a cybersecurity or assessment and authorization (A&A) related ?eld Experience shall include implementing and/or reviewing Risk Mitigation Framework (RMF) and A&A lifecycle documentation in accordance with DON, DoD, NIST SP-800-37, and SP-800-53 Rev 4 policies; ensuring/validating the confidentiality, integrity, and availability of systems, networks, and information; and conducting risk and vulnerability reviews and assessments to ensure accreditation procedures were followed, and documenting non-compliance

MINIMUM IA Workforce Baseline: (1) of the following certifications: CAP, GSLC, Security+ CE

Security Requirement: SECRET Clearance

System Administrator II (SA2)(one resume required):

Target Education: Bachelor's Degree in Electrical/Electronic/Computer Engineering, Computer Science, or Information Systems

Target Experience: Three (3) years of experience with server administration with Windows Server Operating System, SQL server and vulnerability management using tools Experience capturing and refining informatic security operational and security requirements, and ensuring those requirements are properly addressed through purposeful architecting, design, development, and configuration; and implementing security controls, configuration changes, software/hardware updates/patches, vulnerability scanning, and securing configurations

MINIMUM IA Workforce Baseline: (1) of the following certifications: CCNA Security, CySA+ **, GIC SP, G SEC, Security + CE, SSCP Security + CE, SSCP

Security Requirement: SECRET Clearance

Computer Programmer I(14071)(one resume required):

Target Education: Associate's Degree in Computer Science, Information Technology, or an equivalent technical field

Target Experience: Entry Level Computer Programmer who is familiar with computer programming languages and modern web development methodologies

MINIMUM IA Workforce Baseline: (1) of the following certifications: Security+ CE, A+ CE, CCNA-Security, Network+ CE, SSCP

Security Requirement: SECRET Clearance

8.1.2 Non-Key Personnel

Computer Programmer III (14073):

Minimum Education: Bachelor's Degree in Computer Science, Information Technology, or an equivalent technical field

Minimum Experience: Seven (7) years of experience with programming applications and database back ends Experience debugging and correcting software errors in existing systems and developing new systems fror requirements documentation

MINIMUM IA Workforce Baseline: (1) of the following certifications: CCNA Security, CySA+ **, GIC SP, G SEC, Security + CE, SSCP Security + CE, SSCP

Security Requirement: SECRET Clearance

Computer Programmer I (14071):

Minimum Education: Associate's Degree in Computer Science, Information Technology, or an equivalent technical field

Minimum Experience: Entry Level Computer Programmer who is familiar with computer programming languages and modern web development methodologies a plus

MINIMUMIA Workforce Baseline: (1) of the following certifications: Security+ CE, A+ CE, CCNA-Security, Network+ CE, SSCP

Security Requirement: SECRET Clearance

Computer Systems Analyst II (14102):

Minimum Education: Bachelor's Degree in Computer Science, Information Technology, or an equivalent technical field

Minimum Experience: Three (3) years of experience with developing web applications, technical software documentation, database administration, and programming is necessary Experience with Microsoft ASP.NET technologies in addition to experience with C# programming language, MSSQL, Java Script, and HTML 5

MINIMUM IA Workforce Baseline: (1) of the following certifications: CAP, GSLC, Security+ CE

Security Requirement: SECRET Clearance

Specialist, Information Assurance Compliance II (SIAC2):

Minimum Education: Bachelor's Degree in Computer Science, Information Technology, or an equivalent technical field or CNSSI 4012 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CISO certificate or success completion of at least one of the following military training courses: NEC 2780 (CIN: A-531-0022) or 2779 (CIN: A-531-0009) or 2781 (CIN: A-531-0045) (or DOD Service equivalent)

Minimum Experience: Five (5) years' practical experience in a cybersecurity or assessment and authorization (A&A) related field Experience shall include implementing and/or reviewing RMF and A&A lifecycle documentation in accordance with DON, DoD, NIST SP-800-37, and SP-800-53 Rev 4 policies; ensuring/validating the confidentiality, integrity, and availability of systems, networks, and information; and conducting and vulnerability reviews and assessments to ensure accreditation procedures were followed, and documenting non-compliance

MINIMUM IA Workforce Baseline: One (1) of the following certifications: CAP, GSLC, Security+ CE

Security Requirement: SECRET Clearance

Specialist, Information System Security III (SISS3):

Minimum Education: Master's Degree in Computer Science, Information Technology, or an equivalent technical field

Minimum Experience: Eight (8) years of experience coordinating with various levels of an organization to enact required security changes to ensure compliance with published policies; conducting cybersecurity vulnerability and threat analysis; and support cyber-incident-response by isolating potentially effected assets, initial investigation and data collection, through status updates/reporting

MINIMUM IA Workforce Baseline: (1) of the following certifications: CAP, CASP+ CE, CISM, CISSP (or Associate), GSLC, CCISO

Security Requirement: SECRET Clearance

Specialist, Information System Security II (SISS2):

Minimum Education: Bachelor's Degree in Computer Science, Information Technology, or an equivalent technical field

Minimum Experience: Five (5) years of experience coordinating with various levels of an organization to enact required security changes to ensure compliance with published policies; conducting cybersecurity vulnerability and threat analysis; and support cyber-incident-response by isolating potentially effected assets, initial investigation and data collection through status updates/reporting

MINIMUM IA Workforce Baseline: (1) of the following certifications: CAP, GSLC, Security+ CE

Security Requirement: SECRET Clearance

System Administrator II (SA2) :

Minimum Education: Bachelor's Degree in Electrical/Electronic/Computer Engineering, Computer Science, or Information Systems

Minimum Experience: Three (3) years of professional experience capturing and refining information security operational and security requirements, and ensuring those requirements are properly addressed through purposeful architecting, design, development, and configuration; and implementing security controls, configuration changes, software/hardware updates/patches, vulnerability scanning, and securing configurations

MINIMUM IA Workforce Baseline: (1) of the following certifications: CCNA Security, CySA+ **, GIC SP, G SEC, Security + CE, SSCP Security + CE, SSCP

Security Requirement: SECRET Clearance

Machinery Maintenance Mechanic I (23530):

Minimum Education: High School Diploma, trade/industrial school diploma, GED equivalent, or completion of technical or military school course of study in mechanical/electrical/electronic/control systems theory, or completed training on the maintenance and operation of military based technical equipment, specific to Gas Turbine Engines

Minimum Experience: Two (2) years of experience in warehouse inventory including maintaining acceptable and accurate inventory levels; reporting shortages, overages and all inventory levels monthly for replenishn classifying, labeling, locating and warehousing all inventory for future use Two (2) years of experience in assemblage of material designated on packing slips/orders for material; packaging and labeling material for shipment; receiving incoming shipments of material; retrieving packing slips, routing incoming material to cognizant requestor or area; retrieving invoices for signature when necessary; documenting receipt of materia Individual should have familiarity with Windows operating system environment as well as familiarity with Microsoft Outlook, Word and Excel is required

Security Requirement: CONFIDENTIAL Clearance

Machinery Maintenance Mechanic II (23530):

Minimum Education: High school, trade/industrial school diploma, GED equivalent or completion of a technical or military school course of study in mechanical/electrical/electronic/control systems theory or complete training on the maintenance and operation of military based technical equipment, such as Gas Turbine School

Minimum Experience: Three (3) years of experience with internal combustion engine type work including corrective maintenance procedures to restore failed equipment to an operational condition within predetermine parameters (Preferably gas turbine) Familiarity with hand tools and their proper usage, a working knowledge of general maintenance practices, troubleshooting and repair work is required

Security Requirement: CONFIDENTIAL Clearance

Supply Technician (01410):

Minimum Education: High school, trade/industrial school diploma or GED equivalent

Minimum Experience: Two (2) years of experience in warehouse inventory including maintaining acceptable and accurate inventory levels; reporting shortages, overages and all inventory levels monthly for replenishn classifying, labeling, locating and warehousing all inventory for future use Two (2) years' experience in assemblage of material designated on packing slips/orders for material; packaging and labeling material for shipment; receiving incoming shipments of material; retrieving packing slips, routing incoming material to cognizant requestor or area; retrieving invoices for signature when necessary; documenting receipt of materia Familiarity with Windows operating system environment as well as familiarity with Microsoft Outlook, Word and Excel is required

Security Requirement: CONFIDENTIAL Clearance

9.0 NSWCPD ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (ECRAFT) SYSTEM

The contractor agrees to provide supporting accounting system reports, at the Contracting Officer's request, based on the review of the invoice documentation submitted to eCRAFT This documentation will include report such as the Job Summary Report (or equivalent), Labor Distribution Report (or equivalent), and General Ledger Detail Report (or equivalent) Supporting labor data provided must include unburdened direct labor rates fo each employee and labor category Cost breakdowns for ODCs, Materials, travel and other non-labor costs must be at the transactional level in sufficient detail so the Government can review allocability to the contract/tas order Indirect costs allocated to direct costs must be shown at the lowest level of detail sufficient to reconcile each indirect rate to the appropriate allocation base

On invoices containing subcontractor costs, the prime contractor agrees, at the Contracting Officer's request, to attach as supporting documentation all invoices received from subcontractors, unless the subcontractor submits invoices directly to the CO and COR This requirement applies to all subcontract types (Cost, FFP, etc)

10.0 Quality Management System

10 1 The contractor shall:

- Maintain a Quality Management System (QMS) in accordance with ASQ/ANSI/ISO 9001:2015 standards per Naval Sea Systems Command (NAVSEA) QMS Acceptance Authority or appropriate directorate requiren All QMS packages are required to adhere to applicable NAVSEA Technical Specification 9090-310 and NAVSEA Standard Item 009-04 requirements (CDRL A008)
- Notify NSWCPD's Quality Department in writing when any changes are made to the QMS that may affect work defined in accordance with NAVSEA Technical Specification 9090-310
- Submit its QMS Level 3 specific work procedures relevant to the requirements of the Solicitation, including the SOW at the Task Order level (i e welding, etc)

10 2 Risk Management

The contractor shall:

- Perform risk management and security engineering for Zone D boundaries to include IAVM support, remediation, patching, scanning and associated boundary maintenance

Appendix A – Cybersecurity Workforce (CSWF) Label Guidance for the Document Preparer

CSWF Labels are provided below in accordance with SECNAV M-5239 2–

- Identifying the CSWF label will help transitioning to the CSWF requirements when the Navy directs the change
- The proper proficiency level should be chosen for each CSWF label
  - IAWF xxx-I = Entry CSWF
  - IAWF xxx-II = Intermediate CSWF
  - IAWF xxx-III = Advanced CSWF
  - Ex: IAM II = Intermediate
- The CSWF designation should be chosen based on the position responsibilities/description Navy COOL is a quick resource for identifying this: https://www cool navy mil/usn/cswf/index htm
- It is highly recommended that you cross-check requirements for CSWF designation and proficiency with requirements for the IAWF designation This will help with transitioning between the programs
  - Ex: An Entry 41 - Customer Service and Technical Support can meet their requirements via A+, Network+ or SSCP These align directly to someone with an IAWF designation of IAT-I (A+, CCNA-Security, Network+, SSCP)
  - IAWF and CSWF requirements do not always align Do not rely on Navy cool for the most current baseline requirement certification list NAVIFOR provides in Excel format it as "5239 2 Appendix 4" via its site: https://usff navy deps mil/sites/NAVIFOR/manpower/cswf/SitePages/Home aspx

IAWF Designation Requirement (DOD 8570.01-M) Guidance for the Document Preparer

Approved Baseline Certifications		
IAT Level I	**IAT Level II**	**IAT Level III**
A+ CE CCNA-Security CND Network+ CE SSCP	CCNA Security CySA+ ** GICSP GSEC Security+ CE CND SSCP	CASP+CE CCNP Security CISA CISSP (or Associate) GCED GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP CND Cloud+ GSLC Security+ CE	CAP CASP+CE CISM CISSP (or Associate) GSLC CCISO	CISM CISSP (or Associate) GSLC CCISO
IASAE I	**IASAE II**	**IASAE III**
CASP+CE CISSP (or Associate) CSSLP	CASP+CE CISSP (or Associate) CSSLP	CISSP-ISSAP CISSP-ISSEP
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**
CEH CFR CCNA Cyber Ops CCNA Security CySA+ ** GCIA GCIH GICSP Cloud+ SCYBER PenTest+	CEH CySA+ ** GICSP SSCP CHFI CFR Cloud+ CND	CEH CFR CCNA Cyber Ops CCNA Security CHFI CySA+ ** GCFA GCIH SCYBER PenTest+
CSSP Auditor	**CSSP Manager**	
CEH CySA+ ** CISA GSNA CFR PenTest+	CISM CISSP-ISSMP CCISO	

- Baseline certification requirements for the IAWF can be found at: https://public cyber mil/cwmp/dod-approved-8570-baseline-certifications/
- Higher level IAT/IAM/IASAE certifications satisfy lower level requirements Certifications listed in Level II or III cells can be used to qualify for Level I However, Level I certifications cannot be used for Level II or III
- OS/CE Requirements will be determined by systems they need privileged access to They are required to have an actual certification (not a training certificate) for these systems You can determine the correct certification based on your needs The CSWF PM, ISSOs, and ISSM can assist with this as well
- Information Assurance (IA) Management (IAM)
  - Typically personnel in oversight/compliance roles that may:
    - Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered
    - Ensure that system security configuration guidelines are followed
    - Ensure that IA security requirements are appropriately identified in computer environment operation procedures
    - Ensure that IA inspections, tests, and reviews are coordinated
    - Participate in an IS risk assessment during the Assessment and Authorization (A&A) / Risk Management Framework (RMF) process
  - May also carry out IAT duties, as long as they also meet IAT requirements
  - May include information system security officers (ISSOs)
- IA Technicians (IAT)
  - Typically system/network/application administrators doing technical work that may include:
    - Implement applicable patches to remediate vulnerabilities
    - Install, test, maintain, and upgrade CE operating systems software and hardware to comply with cybersecurity requirements
    - Implement and maintain perimeter defense systems including, but not limited to, intrusion detection systems, firewalls, grid sensors
    - Schedule and perform regular and special backups on all enclave systems
    - Examine vulnerabilities and determine actions to mitigate them
- IA System Architects and Engineers (IASAE)
  - Typically developers and programmers, work may include:
    - Design, develop, and implement security measures that provide confidentiality, integrity, availability, authentication, and on-repudiation for the enclave environment
    - Develop interface specifications for use within the enclave environment
    - Develop cybersecurity architectures and designs for DoD IS to include automated IS applications, enclaves (which include networks), and special purpose environments with platform IT interconnectivity, e g , weapons systems, sensors, medical technologies, or distribution systems
    - Provide engineering support to security/certification test and evaluation activities

Additional Guidance for completing Section 12.3 DON Cyberspace IT (Information Technology) / Cybersecurity & Information Assurance Functions and Personnel Requirements

IT levels should be provided for each position.
IT levels are defined in SECNAV M-5510 30 (see chapter 5)

- IT-I – Privileged Access
- IT-I users require a Tier 5 (T5) background investigation (Top Secret eligibility)
- This would typically be used for high-level administrators on centrally managed or cloud-based networks/information systems that connect to the internet or other DoD large networks (e g , SIPRNet, SDREN)
- Information Systems Security Managers (ISSM), ISSOs, or other positions with responsibility for development and administration of cybersecurity programs, to include direction and control of risk analysis and/or threat assessment
- Positions that have major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring and/or management of systems hardware and software
- General rule: IAM-II/III and IAT-III personnel will be here
  - IT-II – Limited Privilege OR sensitive information access
- IT-II users require a Tier 3 (T3) background investigation (Secret eligibility)
- Limited privilege could include privileged access to a stand-alone network or system, or local administrative privileges on a workstation
- (Privilege can also be considered limited if they are under the immediate supervision of an IT-I
- Sensitive information includes sensitive but unclassified (SBU) and controlled unclassified information (CUI) Examples include: Personally Identifiably Information (PII), For Official Use Only (FOUO), Naval Nuclear Propulsion Information (NNPI)

- IT-III – No Privilege AND no sensitive information access
- This category should only be used if personnel will ONLY have access to publically releasable information

C-202-H001 ADDITIONAL DEFINITIONS--BASIC (NAVSEA) (OCT 2018)

(a) Department - means the Department of the Navy

(b) Commander, Naval Sea Systems Command - means the Commander of the Naval Sea Systems Command of the Department of the Navy or his duly appointed successor

(c) References to The Federal Acquisition Regulation (FAR) - All references to the FAR in this contract shall be deemed to also reference the appropriate sections of the Defense FAR Supplement (DFARS), unless clearly indicated otherwise

(d) National Stock Numbers - Whenever the term Federal Item Identification Number and its acronym FIIN or the term Federal Stock Number and its acronym FSN appear in the contract, order or their cited specifications and standards, the terms and acronyms shall be interpreted as National Item Identification Number (NIIN) and National Stock Number (NSN) respectively which shall be defined as follows:

(1) National Item Identification Number (NIIN) The number assigned to each approved Item Identification under the Federal Cataloging Program It consists of nine numeric characters, the first two of which are the National Codification Bureau (NCB) Code The remaining positions consist of a seven digit non-significant number

(2) National Stock Number (NSN) The National Stock Number (NSN) for an item of supply consists of the applicable four-position Federal Supply Class (FSC) plus the applicable nine-position NIIN assigned to the item of supply

C-204-H001 USE OF NAVY SUPPORT CONTRACTORS FOR OFFICIAL CONTRACT FILES (NAVSEA) (OCT 2018)

(a) NAVSEA may use a file room management support contractor, hereinafter referred to as "the support contractor", to manage its file room, in which all official contract files, including the official file supporting this procurement, are retained These official files may contain information that is considered a trade secret, proprietary, business sensitive or otherwise protected pursuant to law or regulation, hereinafter referred to as "protected information" File room management services consist of any of the following: secretarial or clerical support; data entry; document reproduction, scanning, imaging, or destruction; operation, management, or maintenance of paper-based or electronic mail rooms, file rooms, or libraries; and supervision in connection with functions listed herein

(b) The cognizant Contracting Officer will ensure that any NAVSEA contract under which these file room management services are acquired will contain a requirement that:

(1) The support contractor not disclose any information;

(2) Individual employees are to be instructed by the support contractor regarding the sensitivity of the official contract files;

(3) The support contractor performing these services be barred from providing any other supplies and/or services, or competing to do so, to NAVSEA for the period of performance of its contract and for an additional three years thereafter unless otherwise provided by law or regulation; and,

(4) In addition to any other rights the contractor may have, it is a third party beneficiary who has the right of direct action against the support contractor, or any person to whom the support contractor has released or disclosed protected information, for the unauthorized duplication, release, or disclosure of such protected information

(c) Execution of this contract by the contractor is considered consent to NAVSEA's permitting access to any information, irrespective of restrictive markings or the nature of the information submitted, by its file room management support contractor for the limited purpose of executing its file room support contract responsibilities

(d) NAVSEA may, without further notice, enter into contracts with other contractors for these services Contractors should enter into separate non-disclosure agreements with the file room contractor Contact the Procuring Contracting Officer for contractor specifics However, any such agreement will not be considered a prerequisite before information submitted is stored in the file room or otherwise encumber the government

(End of Text)

C-211-H001 ACCESS TO THE VESSEL(S) (NAVSEA) (OCT 2018)

Officers, employees and associates of other prime Contractors with the Government and their subcontractors, shall, as authorized by the Supervisor, have, at all reasonable times, admission to the plant, access to the vessel(s) where and as required, and be permitted, within the plant and on the vessel(s) required, to perform and fulfill their respective obligations to the Government The Contractor shall make reasonable arrangements with the Government or Contractors of the Government, as shall have been identified and authorized by the Supervisor to be given admission to the plant and access to the vessel(s) for office space, work areas, storage or shop areas, or other facilities and services, necessary for the performance of the respective responsibilities involved, and reasonable to their performance

(End of Text)

C-211-H011 USE OF POWER GRINDERS AND SAWS (NAVSEA) (OCT 2018)

(a) All portable pneumatic grinders or reciprocating saws that are to be used on reactor plant material or equipment or used within the reactor compartment shall be equipped with safety lock-off devices In addition, the Contractor agrees that all portable pneumatic grinders or reciprocating saws that it purchases or acquires subsequent to the date of this contract, for use in performance of this contract in Naval workplace areas shall be equipped with safety lock-off devices

(b) A "safety lock-off device" is any operating control which requires positive action by the operator before the tool can be turned on The lock-off device shall automatically and positively lock the throttle in the off position when the throttle is released Two consecutive operations by the same hand shall be required first to disengage the lock-off device and then to turn on the throttle The lock-off device shall be integral with the tool, shall not adversely affect the safety or operating characteristics of the tool, and shall not be easily removable

(c) Devices, such as a "dead man control" or "quick-disconnect", which do not automatically and positively lock the throttle in the off position when the throttle is released, are not safety lock-off devices

(End of Text)

C-211-H016 SPECIFICATIONS AND STANDARDS (NAVSEA) (OCT 2018)

(a) Definitions

(i) A "zero-tier reference" is a specification, standard, or drawing that is cited in the contract (including its attachments)

(ii) A "first-tier reference" is either: (1) a specification, standard, or drawing cited in a zero-tier reference, or (2) a specification cited in a first-tier drawing

(b) Requirements All zero-tier and first-tier references, as defined above, are mandatory for use All lower tier references shall be used for guidance only unless specifically identified below

NONE

(End of Text)

C-211-H017 UPDATING SPECIFICATIONS AND STANDARDS (NAVSEA) (DEC 2018)

The contractor may request that this contract be updated to include the current version of the applicable specification or standard if the update does not affect the form, fit or function of any deliverable item or increase the cost/price of the item to the Government The contractor should submit update requests to the Procuring Contracting Officer with copies to the Administrative Contracting Officer and cognizant program office representative for approval The contractor shall perform the contract in accordance with the existing specifications and standards until notified of approval/disapproval of its request to update by the Procuring Contracting Officer Any approved alternate specifications or standards will be incorporated into the contract

(End of Text)

C-211-H018 APPROVAL BY THE GOVERNMENT (NAVSEA) (JAN 2019)

Approval by the Government as required under this contract and applicable specifications shall not relieve the Contractor of its obligation to comply with the specifications and with all other requirements of the contract, nor shall it impose upon the Government any liability it would not have had in the absence of such approval

(End of Text)

C-211-H020 PROTECTION OF THE VESSEL (NAVSEA) (MAR 2019)

(a) The Contractor shall exercise reasonable care, as agreed upon with the Supervisor, to protect the vessel from fire, and shall maintain a system of inspection over the activities of its welders, burners, riveters, painters, pipe fitters, and similar workers, and of its subcontractors, particularly where such activities are undertaken in the vicinity of the vessel's magazines, fuel oil tanks, or store rooms containing inflammable materials All ammunition, fuel oil, motor fuels, and cleaning fluids shall have been off-loaded and the tanks cleaned, except as may be mutually agreed upon between the Contractor and the Supervisor prior to work on the vessel by the Contractor Fire hose lines shall be maintained by the Contractor ready for immediate use on the vessel at all times while the vessel is berthed alongside the Contractor's pier or in dry dock All tanks under alteration or repair shall be cleaned, washed, and steamed out or otherwise made safe to the extent necessary, and the Contractor shall furnish the vessel's Gas Free Officer and the Supervisor with a "Gas Chemists' Certificate" before any hot work is done The Contractor shall maintain a fire watch aboard the vessel in areas where the Contractor is working All other fire watches aboard the vessel shall be the responsibility of the Government

(b) Except as otherwise provided in contractually invoked technical specifications or NAVSEA furnished directives, while the vessel is at the Contractor's plant and when the temperature becomes as low as thirty-five degrees Fahrenheit, the Contractor shall assist the Government when requested in keeping all pipe-lines, fixtures, traps, tanks, and other receptacles on the vessel drained to avoid damage from freezing, or if this is not practicable, the vessel shall be kept heated to prevent such damage The vessel's stern tube and propeller hubs shall be protected by the Contractor from frost damage by applied heat through the use of a salamander or other proper means

(c) The work shall, whenever practicable, be performed in such manner as not to interfere with the work performed by military personnel attached to the vessel, and provisions shall be made so that personnel assigned shall have access to the vessel at all times, it being understood that such personnel will not unduly interfere with the work of the Contractor's workmen

(d) The Contractor shall at all times keep the site of the work on the vessel free from accumulation of waste material or rubbish caused by its employees, or the work performed by the Contractor in accordance with this contract, and at the completion of such work shall remove all rubbish from and about the site of the work, and shall leave the work in its immediate vicinity "broom clean", unless more exactly specified by the Supervisor

(End of Text)

C-215-H002 CONTRACTOR PROPOSAL (NAVSEA) (OCT 2018)

(a) Performance of this contract by the Contractor shall be conducted and performed in accordance with detailed obligations to which the Contractor committed itself in Proposal dated 15 January 2021 in response to NAVSEA Solicitation No N64498-20-R-3010

(b) The technical volume(s) of the Contractor's proposal is(are) hereby incorporated by reference and made subject to the "Order of Precedence" (FAR 52 215-8) clause of this contract Under the "Order of Precedence" clause, the technical volume(s) of the Contractor's proposal referenced herein is (are) hereby designated as item (f) of the clause, following "the specifications" in the order of precedence

C-222-H001 ACCESS TO THE VESSELS BY NON-U.S. CITIZENS (NAVSEA) (APR 2019)

(a) No person not known to be a U S citizen shall be eligible for access to naval vessels, work sites and adjacent areas when said vessels are under construction, conversion, overhaul, or repair, except upon a finding by COMNAVSEA or his designated representative that such access should be permitted in the best interest of the United States The Contractor shall establish procedures to comply with this requirement and NAVSEAINST 5510 2D

(b) If the Contractor desires to employ non-U S citizens in the performance of work under this contract or agreement that requires access as specified in paragraph (a) of this requirement, approval must be obtained prior to access for each contract or agreement where such access is required To request such approval for non-U S citizens of friendly countries, the Contractor shall submit to the cognizant Contract Administration Office (CAO), an Access Control Plan (ACP) which shall contain as a minimum, the following information:

(1) Badge or Pass oriented identification, access, and movement control system for non-U S citizen employees with the badge or pass to be worn or displayed on outer garments at all times while on the Contractor's facilities and when performing work aboard ship

(i) Badges must be of such design and appearance that permits easy recognition to facilitate quick and positive identification

(ii) Access authorization and limitations for the bearer must be clearly established and in accordance with applicable security regulations and instructions

(iii) A control system, which provides rigid accountability procedures for handling lost, damaged, forgotten or no longer required badges, must be established

(iv) A badge or pass check must be performed at all points of entry to the Contractor's facilities or by a site supervisor for work performed on vessels outside the Contractor's plant

(2) Contractor's plan for ascertaining citizenship and for screening employees for security risk

(3) Data reflecting the number, nationality, and positions held by non-U S citizen employees, including procedures to update data as non-U S citizen employee data changes, and pass to cognizant CAO

(4) Contractor's plan for ensuring subcontractor compliance with the provisions of the Contractor's ACP

(5) These conditions and controls are intended to serve as guidelines representing the minimum requirements of an acceptable ACP They are not meant to restrict the Contractor in any way from imposing additional controls necessary to tailor these requirements to a specific facility

(c) To request approval for non-U S citizens of hostile and/or communist-controlled countries (listed in Department of Defense Industrial Security Manual, DOD 5220 22-M or available from cognizant CAO), Contractor shall include in the ACP the following employee data: name, place of birth, citizenship (if different from place of birth), date of entry to U S , extenuating circumstances (if any) concerning immigration to U S , number of years employed by Contractor, position, and stated intent concerning U S citizenship COMNAVSEA or his designated representative will make individual determinations for desirability of access for the above group Approval of ACP's for access of non-U S citizens of friendly countries will not be delayed for approval of non-U S citizens of hostile communist-controlled countries Until approval is received, Contractor must deny access to vessels for employees who are non-U S citizens of hostile and/or communist-controlled countries

(d) The Contractor shall fully comply with approved ACPs Noncompliance by the Contractor or subcontractor serves to cancel any authorization previously granted, in which case the Contractor shall be precluded from the continued use of non-U S citizens on this contract or agreement until such time as the compliance with an approved ACP is demonstrated and upon a determination by the CAO that the Government's interests are protected Further, the Government reserves the right to cancel previously granted authority when such cancellation is determined to be in the Government's best interest Use of non-U S citizens, without an approved ACP or when a previous authorization has been canceled, will be considered a violation of security regulations Upon confirmation by the CAO of such violation, this contract, agreement or any job order issued under this agreement may be terminated for default in accordance with the clause entitled "Default (Fixed-Price Supply And Service)" (FAR 52 249-8), "Default (Fixed-Price Research And Development)" (FAR 52 249-9) or "Termination (Cost Reimbursement)" (FAR 52 249-6), as applicable

(e) Prime Contractors have full responsibility for the proper administration of the approved ACP for all work performed under this contract or agreement, regardless of the location of the vessel, and must ensure compliance by all subcontractors, technical representatives and other persons granted access to U S Navy vessels, adjacent areas, and work sites

(f) In the event the Contractor does not intend to employ non-U S citizens in the performance of the work under this contract, but has non-U S citizen employees, such employees must be precluded from access to the vessel and its work site and those shops where work on the vessel's equipment is being performed The ACP must spell out how non-U S citizens are excluded from access to contract work areas

(g) The same restriction as in paragraph (f) above applies to other non-U S citizens who have access to the Contractor's facilities (e g , for accomplishing facility improvements, from foreign crewed vessels within its facility, etc) except that, with respect to access to the vessel and worksite, the restrictions shall not apply to uniformed U S Navy personnel who are non-U S citizens and who are either assigned to the ship or require access to the ship to perform their duties

(End of Text)

C-223-H004 MANAGEMENT AND DISPOSAL OF HAZARDOUS WASTE (NAVSEA) (MAR 2019)

(a) General

(1) The Contractor shall comply with the Resource Conservation and Recovery Act (RCRA), the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (CERCLA), 10 U S C 7311 and all other applicable Federal, State and local laws, codes, ordinances and regulations for the management and disposal of hazardous waste

(2) Nothing contained in this special contract requirement shall relieve the Contractor from complying with applicable Federal, State, and local Laws, codes, ordinances, and regulations, including obtaining licenses and permits, giving notices and submitting reports, in connection with hazardous waste management and disposal in the performance of this contract Nothing contained herein shall serve to alter either party's liability or responsibility under CERCLA

(3) Materials contained in ship systems are not waste until after removal from the system

(b) Identification of Hazardous Wastes - _____ of this contract identifies the types and amounts of hazardous wastes that are required to be removed by the Contractor, or that are expected to be generated, during the performance of work under this contract

(c) Generator Identification Numbers

(1) Documentation related to hazardous waste generated solely by the physical actions of ship's force or Navy employees on board the vessel shall only bear a generator identification number issued to the Navy pursuant to applicable law

(2) Documentation related to hazardous waste generated solely by the physical actions of Contractor personnel shall only bear a generator identification number issued to the Contractor pursuant to applicable law Regardless of the presence of other materials in or on the shipboard systems or structures which may have qualified a waste stream as hazardous, where the Contractor performs work on a system or structure using materials (whether or not the use of such materials was specified by the Navy) which by themselves would cause the waste from such work to be a hazardous waste, documentation related to such waste shall only bear a generator identification number issued to the Contractor

(3) Documentation related to hazardous waste generated by the combined physical actions of Navy and Contractor personnel shall bear a generator identification number issued to the Contractor pursuant to applicable law and shall also cite in the remarks block a generator identification number issued to the Navy pursuant to applicable law

(4) Notwithstanding paragraphs (c)(1) - (c)(3) above, hazardous wastes are considered to be co-generated in cases where: (a) the Contractor merely drains a system and such drainage creates hazardous waste or

(b) the Contractor performs work on a system or structure using materials which by themselves would not cause the waste from such work to be hazardous waste but such work nonetheless creates a hazardous waste Documentation related to such co-generated waste shall bear a generator identification number in accordance with the provisions of paragraph (c)(3) above

(5) In the event of a failure by the parties to agree to the assignment of a generator identification number to any hazardous waste as set forth in paragraphs (c)(1) through (c)(4) above, the Government may direct which party or parties shall provide generator identification numbers for the waste and such number(s) shall be used on all required documentation Any disagreement with this direction shall be a dispute within the meaning of clause of this contract entitled "Disputes" (FAR 52 233-1) However, the Contractor shall not stop any work but shall continue with performance of all work under this contract as specified in the "DISPUTES" clause

(6) Hazardous Waste Manifests - For wastes described in (c)(2), (c)(3), and (c)(4) above (and (c)(5) as applicable), the Contractor shall sign the generator certification on the Uniform Hazardous Waste Manifest whenever use of the Manifest is required for disposal The Contractor shall obtain _____ concurrence with the categorization of wastes under paragraphs (c)(3) and (c)(4) above before completion of the manifest Manifests prepared pursuant to paragraph (c)(1) above shall be presented to the for completion after the hazardous waste has been identified

(7) For purposes of paragraphs (c)(2) and (3) herein, if the Contractor, while performing work at a Government facility, cannot obtain a separate generator identification number from the State in which the availability will be performed, the Contractor shall notify _____ within 3 business days of receipt of written notification by the State After obtaining _____ approval, the Contractor shall use the Navy site generator identification number and insert in the remarks block the contractor generator identification number issued for the site where his main facilities are located For purposes of paragraph (c)(1) herein, if the work is being performed at a contractor facility and the Government cannot obtain a separate generator identification number for the State, the Government shall use the Contractor site generator identification number and shall cite in the remarks block a Navy generator identification number In both instances described above, the Contractor shall prepare the Uniform Hazardous Waste Manifest described in paragraph (c)(6) above and present it to _____ for completion

(End of Text)

C-223-W002 ON-SITE SAFETY REQUIREMENTS (NAVSEA) (OCT 2018)

(a) The contractor shall ensure that each contractor employee reads any necessary safety documents within 30 days of commencing performance at any Government facility Required safety documents can be obtained from the respective safety office Contractors shall notify the Safety office points of contact below to report completion of the required training via email The email shall include the contractor employee's name, work site, and contract number

(b) It is expected that contractor employees will have received training from their employer on hazards associated with the areas in which they will be working and know what to do in order to protect themselves Contractors are required to adhere to the requirements of 29 CFR 1910, 29 CFR 1926 and applicable state and local requirements while in Government spaces The contractor shall ensure that all on-site contractor work at the Government facility is in accordance with any local safety instructions as provided via the COR The contractor shall report all work-related injuries/illnesses that occurred while working at the Government site to the COR

(c) Contractors whose employees perform work within Government spaces in excess of 1000 hours per calendar quarter during a calendar year shall submit the data elements on OSHA Form 300A, Summary of Work Related Injuries and Illnesses, for those employees to the safety office, via the COR by 15 January for the previous calendar year, even if no work related injuries or illnesses occurred If a contractor's injury/illness rates are above the Bureau of Labor Statistics industry standards, a safety assessment may be performed by the Safety Office to determine if any administrative or engineering controls can be utilized to prevent further injuries/illnesses, or if any additional Personal Protective Equipment or training will be required

(d) Any contractor employee exhibiting unsafe behavior may be removed from the Government site Such removal shall not relieve the contractor from meeting its contractual obligations and shall not be considered an excusable delay as defined in FAR 52 249-14

(e) The Safety Office points of contacts are as follows: Paul Breeden; Paul Breedan@navy mil

(End of Text)

C-227-H006 DATA REQUIREMENTS (NAVSEA) (OCT 2018)

The data to be furnished hereunder shall be prepared in accordance with the Contract Data Requirements List, DD Form 1423, Exhibit A, attached hereto

Contract Status Report (CDRL A001)
Travel Report (CDRL A002)
Contractor's Personnel Roster (CDRL A003)
Other Direct Cost Report (A004)
Software Components Report (CDRL A005)
Contract Financial Analysis Report (CDRL A006)
Risk Management Framework (RMF) Report (CDRL A007)
Quality Management System (QMS) Manual (CDRL A008)

C-227-H008 GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM (NAVSEA) (DEC 2018)

(a) The contractor shall actively participate in the Government Industry Data Exchange Program in accordance with the GIDEP Operations Manual, S0300-BT-PRO-010 The contractor shall submit information concerning critical or major nonconformances, as defined in FAR 46 407/DFARS 246 407, to the GIDEP information system

(b) The contractor shall insert paragraph (a) of this clause in any subcontract when deemed necessary When so inserted, the word "contractor" shall be changed to "subcontractor "

(c) The contractor shall, when it elects not to insert paragraph (a) in a subcontract, provide the subcontractor any GIDEP data which may be pertinent to items of its manufacture and verify that the subcontractor utilizes any such data

(d) The contractor shall, whether it elects to insert paragraph (a) in a subcontract or not, verify that the subcontractor utilizes and provides feedback on any GIDEP data that may be pertinent to items of its manufacture "

(e) GIDEP materials, software and information are available without charge from:

GIDEP Operations Center
P O Box 8000
Corona, CA 92878-8000
Phone: (951) 898-3207
FAX: (951) 898-3250
Internet: http://www gidep org

(End of Text)

C-227-H010 COMPUTER SOFTWARE AND COMPUTER DATA BASES DELIVERED TO OR RECEIVED FROM THE GOVERNMENT (NAVSEA) (JAN 2019)

(a) The Contractor agrees to test for viruses, malware, Trojan Horses, and other security threats such as those listed in NIST Special Publication 800-12 Rev 1, An Introduction to Computer Security, The NIST Handbook, Chapter 4, in all computer software and computer data bases (as defined in the clause entitled "Rights In Noncommercial Computer Software and Noncommercial Computer Software Documentation" (DFARS 252 227-7014)), before delivery of that computer software or computer data base in whatever media and on whatever system the computer software or data base is delivered whether delivered separately or imbedded

within delivered equipment The Contractor warrants that when delivered any such computer software and computer data base shall be free of viruses, malware, Trojan Horses, and other security threats such as those listed in NIST Special Publication 800-12 Rev 1

(b) The Contractor agrees that prior to use under this contract, it shall test any computer software and computer data base received from the Government for viruses, malware, Trojan Horses, and other security threats listed in NIST Special Publication 800-12 Rev 1, An Introduction to Computer Security, The NIST Handbook, Chapter 4

(c) Any license agreement governing the use of any computer software or computer software documentation delivered to the Government as a result of this contract must be paid-up, irrevocable, world-wide, royalty-free, perpetual and flexible (user licenses transferable among Government employees and personnel under Government contract)

(d) The Contractor shall not include or permit to be included any routine to enable the contractor or its subcontractor(s) or vendor(s) to disable the computer software or computer data base after delivery to the Government

(e) No copy protection devices or systems shall be used in any computer software or computer data base delivered under this contract with unlimited or Government purpose rights (as defined in DFARS 252 227-7013 and 252 227-7014) to restrict or limit the Government from making copies

(f) It is agreed that, to the extent that any technical or other data is computer software by virtue of its delivery in digital form, the Government shall be licensed to use that digital-form data with exactly the same rights and limitations as if the data had been delivered as hard copy

(g) Any limited rights legends or other allowed legends placed by a Contractor on technical data or other data delivered in digital form shall be digitally included on the same media as the digital-form data and must be associated with the corresponding digital-form technical data to which the legend(s) apply to the extent possible Such legends shall also be placed in human-readable form on a visible surface of the media carrying the digital-form data as delivered, to the extent possible

(End of Text)

C-228-H001 INDEMNIFICATION FOR ACCESS TO VESSEL (NAVSEA) (DEC 2018)

Notwithstanding any provision in the "Access to Vessel" clause (DFARS 252 217- 7011), or any other clause of the contract, the Contractor agrees to allow officers, employees, and associates of the Government, or other prime contractors with the Government and their subcontractors, and officers, employees, and associates of offerors on other contemplated work, admission to the Contractor's facilities and access to the vessel without any further request for indemnification from any party, which has not been previously included in the contract price

(End of Text)

C-233-H001 DOCUMENTATION OF REQUESTS FOR EQUITABLE ADJUSTMENT--BASIC (NAVSEA) (OCT 2018)

(a) For the purposes of this special contract requirement, the term "change" includes not only a change that is made pursuant to a written order designated as a "change order" but also (1) an engineering change proposed by the Government or by the Contractor and (2) any act or omission to act on the part of the Government in respect of which a request is made for equitable adjustment

(b) Whenever the Contractor requests or proposes an equitable adjustment of $100,000 or more per vessel in respect to a change made pursuant to a written order designated as a "change order" or in respect to a proposed engineering change and whenever the Contractor requests an equitable adjustment in any amount in respect to any other act or omission to act on the part of the Government, the proposal supporting such request shall contain the following information for each individual item or element of the request:

(1) A description (i) of the work required by the contract before the change, which has been deleted by the change, and (ii) of the work deleted by the change which already has been completed The description is to include a list of components, equipment, and other identifiable property involved Also, the status of manufacture, procurement, or installation of such property is to be indicated Separate description is to be furnished for design and production work Items of raw material, purchased parts, components and other identifiable hardware, which are made excess by the change and which are not to be retained by the Contractor, are to be listed for later disposition;

(2) Description of work necessary to undo work already completed which has been deleted by the change;

(3) Description of work not required by the terms hereof before the change, which is substituted or added by the change A list of components and equipment (not bulk materials or items) involved should be included Separate descriptions are to be furnished for design work and production work;

(4) Description of interference and inefficiencies in performing the change;

(5) Description of each element of disruption and exactly how work has been, or will be disrupted:

(i) The calendar period of time during which disruption occurred, or will occur;
(ii) Area(s) aboard the vessel where disruption occurred, or will occur;
(iii) Trade(s) disrupted, with a breakdown of man-hours for each trade;
(iv) Scheduling of trades before, during, and after period of disruption;
(v) Description of measures taken to lessen the disruptive effect of the change;

(6) Delay in delivery attributable solely to the change;

(7) Other work attributable to the change;

(8) Supplementing the foregoing, a narrative statement of the direct "causal" relationship between any alleged Government act or omission and the claimed consequences therefor, cross-referenced to the detailed information provided as required above; and

(9) A statement setting forth a comparative enumeration of the amounts "budgeted" for the cost elements, including the material costs, labor hours and pertinent indirect costs, estimated by the Contractor in preparing its initial and ultimate proposal(s) for this contract, and the amounts claimed to have been incurred and/or projected to be incurred corresponding to each such "budgeted cost" elements

(c) Each proposal in excess of $100,000 submitted in support of a claim for equitable adjustment under any requirement of this contract shall, in addition to the information required by paragraph (b) hereof, contain such information as the Contracting Officer may require with respect to each individual claim item

(d) It is recognized that individual claims for equitable adjustment may not include all of the factors listed in paragraph (b) above Accordingly, the Contractor is required to set forth in its proposal information only with respect to those factors which are comprehended in the individual claim for equitable adjustment In any event, the information furnished hereunder shall be in sufficient detail to permit the Contracting Officer to cross-reference the claimed increased costs, or delay in delivery, or both, as appropriate, submitted pursuant to paragraph (c) of this requirement, with the information submitted pursuant to paragraph (b) hereof

(End of Text)

C-237-H001 ENTERPRISE-WIDE CONTRACTOR MANPOWER REPORTING APPLICATION (NAVSEA) (OCT 2018)

(a) The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the NSWCPD via a secure data collection site Contracted services excluded from reporting are based on Product Service Codes (PSCs) The excluded PSCs are:

(1) W, Lease/Rental of Equipment;
(2) X, Lease/Rental of Facilities;
(3) Y, Construction of Structures and Facilities;
(4) D, Automatic Data Processing and Telecommunications, IT and Telecom- Telecommunications Transmission (D304) and Internet (D322) ONLY;

(5) S, Utilities ONLY;
(6) V, Freight and Shipping ONLY \
(b) The contractor is required to completely fill in all required data fields using the following web address https://www ecmra mil

(c) Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30 While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year Contractors may direct questions to the help desk, linked at https://dod ecmra support desk@mail mil

(End of Text)

C-237-H002 SUBSTITUTION OF KEY PERSONNEL (NAVSEA) (OCT 2018)

(a) The Contractor agrees that a partial basis for award of this contract is the list of key personnel proposed Accordingly, the Contractor agrees to assign to this contract those key persons whose resumes were submitted with the proposal necessary to fulfill the requirements of the contract No substitution shall be made without prior notification to and concurrence of the Contracting Officer in accordance with this requirement Substitution shall include, but not be limited to, subdividing hours of any key personnel and assigning or allocating those hours to another individual not approved as key personnel

(b) All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced The Contracting Officer shall be notified in writing of any proposed substitution at least forty-five (45) days, or ninety (90) days if a security clearance is to be obtained, in advance of the proposed substitution Such notification shall include: (1) an explanation of the circumstances necessitating the substitution; (2) a complete resume of the proposed substitute; (3) an explanation as to why the proposed substitute is considered to have equal or better qualifications than the person being replaced; (4) payroll record of the proposed replacement; and (5) any other information requested by the Contracting Officer to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award

(c) Key personnel are identified in an attachment in Section J

(End of Text)

C-237-W001 ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (eCRAFT) SYSTEM REPORTING (NAVSEA) (MAY 2019)

(a) The Contractor agrees to upload the Contractor's Funds and Man-hour Expenditure Reports in the Electronic Cost Reporting and Financial Tracking (eCRAFT) System and submit the Contractor's Performance Report on the day and for the same timeframe the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system Compliance with this requirement is a material requirement of this contract Failure to comply with this requirement may result in contract termination

(b) The Contract Status Report indicates the progress of work and the status of the program and of all assigned tasks It informs the Government of existing or potential problem areas

(c) The Contractor's Fund and Man-hour Expenditure Report reports contractor expenditures for labor, materials, travel, subcontractor usage, and other contract charges

(1) Access: eCRAFT: Reports are uploaded through the eCRAFT System Periodic Report Utility (EPRU) The EPRU spreadsheet and user manual can be obtained at: http://www navsea navy mil/Home/Warfare-Centers /NUWC-Newport/Partnerships/Commercial-Contracts/Information-eCraft-/ under eCRAFT information The link for eCRAFT report submission is: https://www pdrep csd disa mil/pdrep_files/other/ecraft htm If you have problems uploading reports, please see the Frequently Asked Questions at the site address above

(2) Submission and Acceptance/Rejection: Submission and Acceptance/Rejection: The contractor shall submit their reports on the same day and for the same timeframe the contractor submits an invoice in WAWF The amounts shall be the same eCRAFT acceptance/rejection will be indicated by e-mail notification from eCRAFT

(End of Text)

C-242-H001 EXPEDITING CONTRACT CLOSEOUT (NAVSEA) (OCT 2018)

(a) As part of the negotiated fixed price or total estimated amount of this contract, both the Government and the Contractor have agreed to waive any entitlement that otherwise might accrue to either party in any residual dollar amount of $1,000 or less at the time of final contract closeout The term "residual dollar amount" shall include all money that would otherwise be owed to either party at the end of the contract, except that, amounts connected in any way with taxation, allegations of fraud and/or antitrust violations shall be excluded For purposes of determining residual dollar amounts, offsets of money owed by one party against money that would otherwise be paid by that party may be considered to the extent permitted by law

(b) This agreement to waive entitlement to residual dollar amounts has been considered by both parties It is agreed that the administrative costs for either party associated with collecting such small dollar amounts could exceed the amount to be recovered

(End of Text)

C-242-H002 POST AWARD MEETNG (NAVSEA) (OCT 2018)

(a) A post-award meeting with the successful offeror will be conducted within thirty (30) days after award of the Task Order The meeting will be virtual

(b) The contractor will be given seven (7) working days' notice prior to the date of the meeting by the Contracting Officer

(c) The requirement for a post-award meeting shall in no event constitute grounds for excusable delay by the contractor in performance of any provisions in the Task Order

(d) The post-award meeting will include, but is not limited to, the establishment of work level points of contact, determining the administration strategy, roles and responsibilities, and ensure prompt payment and close out Specific topics shall be mutually agreed to prior to the meeting

(End of Text)

C-242-H003 TECHNICAL INSTRUCTIONS (NAVSEA) (OCT 2018)

(a) Performance of the work hereunder may be subject to written technical instructions signed by the Contracting Officer and the Contracting Officer's Representative specified in Section G of this contract As used herein, technical instructions are defined to include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work

(2) Guidelines to the Contractor which assist in the interpretation of drawings, specifications or technical portions of work description

(b) Technical instructions must be within the general scope of work stated in the contract Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "CHANGES" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract

(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such instruction The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract

(d) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction
(End of Text)

C-244-H002 SUBCONTRACTORS/CONSULTANTS (NAVSEA) (Jun 202020)

Subcontracts (Jun 2020)
(a) *Definitions* As used in this clause-

"Approved purchasing system" means a Contractor's purchasing system that has been reviewed and approved in accordance with part 44 of the Federal Acquisition Regulation (FAR)
"Consent to subcontract" means the Contracting Officer's written consent for the Contractor to enter into a particular subcontract
Subcontract means any contract, as defined in FAR subpart 2 1, entered into by a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders

(b) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (c) or (d) of this clause

(c) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that-

(1) Is of the cost-reimbursement, time-and-materials, or labor-hour type; or
(2) Is fixed-price and exceeds-

(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold, as defined in FAR 2 101 on the date of subcontract award, or 5 percent of the total estimated cost of the contract; or
(ii) For a contract awarded by a civilian agency other than the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold, as defined in FAR 2 101 on the date of subcontract award, or 5 percent of the total estimated cost of the contract

(d) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before placing the following subcontracts:

(e)

(1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (b), (c), or (d) of this clause, including the following information:

(i) A description of the supplies or services to be subcontracted
(ii) Identification of the type of subcontract to be used
(iii) Identification of the proposed subcontractor
(iv) The proposed subcontract price
(v) The subcontractor's current, complete, and accurate certified cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions
(vi) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract
(vii) A negotiation memorandum reflecting-

(A) The principal elements of the subcontract price negotiations;
(B) The most significant considerations controlling establishment of initial or revised prices;
(C) The reason certified cost or pricing data were or were not required;

(D) The extent, if any, to which the Contractor did not rely on the subcontractor's certified cost or pricing data in determining the price objective and in negotiating the final price;

(E) The extent to which it was recognized in the negotiation that the subcontractor's certified cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;

(F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and

(G) A complete explanation of the incentive fee or profit plan when incentives are used The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered

(2) The Contractor is not required to notify the Contracting Officer in advance of entering into any subcontract for which consent is not required under paragraph (b), (c), or (d) of this clause

(f) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination-

(1) Of the acceptability of any subcontract terms or conditions;
(2) Of the allowability of any cost under this contract; or
(3) To relieve the Contractor of any responsibility for performing this contract

(g) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of-cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15 404-4(c)(4)(i)

(h) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government

(i) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR subpart 44 3

(j) Paragraphs (c) and (e) of this clause do not apply to the following subcontracts, which were evaluated during negotiations:

- (b)(6) [redacted]
- (b)(6) [redacted]
- (b)(6) [redacted]

(End of clause)

C-247-H001 PERMITS AND RESPONSIBILITIES (NAVSEA) (DEC 2018)

The Contractor shall, without additional expense to the Government, be responsible for obtaining any necessary licenses and permits for complying with any applicable Federal, State, and Municipal laws, codes, and regulations for shipping and transportation including, but not limited to, any movement over public highways of overweight/over dimensional materials

(End of Text)